PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 12/12, 29/06, G06F 9/46 — A1

(11) International Publication Number: WO 00/65774

(43) International Publication Date: 2 November 2000 (02.11.00)

(21) International Application Number: PCT/GB00/01465

(22) International Filing Date: 17 April 2000 (17.04.00)

(30) Priority Data:
09/299,954 26 April 1999 (26.04.99) US

(71) Applicant: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant *(for MC only)*: IBM UNITED KINGDOM LIMITED [GB/GB]; P.O. Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

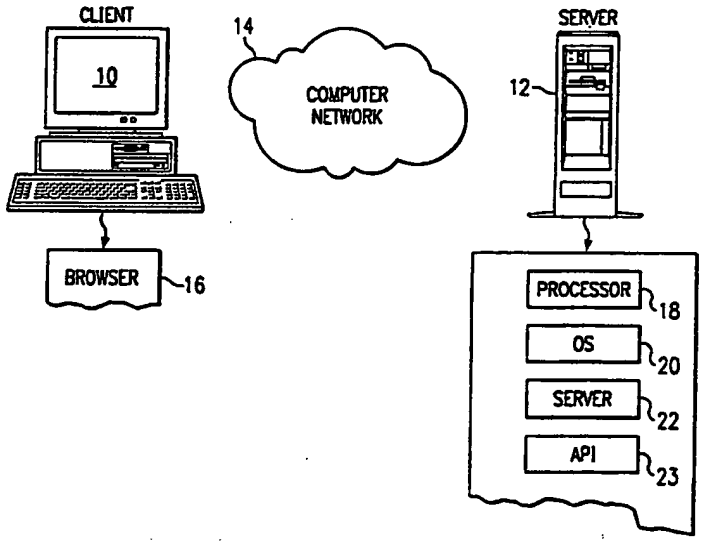
(72) Inventors: BERSTIS, Viktors; 5104 Cuesta Verde, Austin, TX 78746 (US). RODRIGUEZ, Herman; 5309 Ankara Court, Austin, TX 78730 (US).

(74) Agent: DAVIES, Simon, Robert; IBM United Kingdom Limited, Intellectual Property Department, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: REMOTE CONTROL OF A DEVICE



(57) Abstract

A user of a remote computer accesses a target computer (e.g., the user's home PC) via the Internet. To initiate the protocol, the user launches an application which, via the Internet, sends a special request to the user's home e-mail address. If the home computer is not currently connected to the Internet, the user's Internet Service Provider (ISP) dials a telephone number for the home computer. The home computer automatically answers, and the ISP sends authentication information to the computer to establish an Internet connection. With the connection established, an IP address is sent back to the user, which can then be used to invoke X-10 functions, telnet sessions, or other activities with the target computer.

BNSDOCID: <WO___0065774A1_I_>

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

BNSDOCID: <WO___0065774A1_I_>

REMOTE CONTROL OF A DEVICE

Technical Field

This invention relates generally to control of electronic and other devices from a remote location, for example to allow a user to communicate with a home computer via the Internet to control a device at the user's home.

Description of the Related Art

Systems for controlling electrical devices remotely are well known in the prior art. In the past, electrical devices such as lights, motors, HVAC systems, security systems, and the like, have been controlled through radio frequency links. More recently, it has been proposed to connect one's home computer to a home control system conforming to the X-10 initiative. The X-10 protocol is a method to control a set of home devices with a command interface device without the need of physical wiring between the devices. Rather, existing powerlines are used to transmit commands to the receiving devices. In such systems, the user's home computer is connected to the X-10 interface through a serial port connection. Thus, the home computer can be used to control the X-10 interface and, indirectly, the actual physical devices.

It has also been proposed to connect an X-10 system to the Internet to allow a user to monitor his or her home from work or anywhere else using a conventional network connection. These proposals, however, call for a live Internet connection to the user's home computer. A dedicated connection between the user and the home computer is costly both to the user and to the network, and Internet service providers typically have only a limited number of connection ports.

BRIEF SUMMARY OF THE INVENTION

Accordingly the invention provides a method for enabling a remote machine having access to a computer network to control a computer normally connected to the network via a service provider, comprising the steps of: initiating a service request from the remote machine to the computer; responsive to the service request, establishing a network connection between the service provider and the computer; and controlling the computer from the remote machine over the network connection.

BNSDOCID: <WO___0065774A1_I_>

In a further aspect, the invention provides a computer connectable to an Internet Service Provider (ISP) for remotely controlling a device in a home, comprising:

a processor;

a home control application including means for generating a display interface for use in controlling the device; and

a control program executed by the processor comprising:

means for issuing a service request;

means for receiving an IP address identifying a network location;

means for registering the IP address to the home control application; and

means for controlling the home control application to issue a control command to remotely control the device.

In a yet further aspect, the invention provides a computer connectable to an Internet Service Provider (ISP) for controlling a device in a home, comprising:

a processor;

a modem;

a home control application for controlling the device; and

a control program executed by the processor comprising:

means, responsive to an interrupt at the modem, for switching to a given communications

mode;

means for executing a login sequence to the ISP; and

means, responsive to receipt of a control command, for controlling the remote device

through the home control application.

In a yet still further aspect, the invention provides a computer operable at an Internet Service Provider (ISP), comprising:

a processor;

a control program executed by the processor comprising:

means, responsive to a service request from a remote computer, for contacting a target

computer;

means for executing a login sequence with the target computer;

means for issuing an IP address to the target computer if the login sequence is successful; and

means for providing the IP address to the remote computer to enable a user of the remote computer to control a device associated with the target computer.

According to another aspect, the invention provides a computer program product in a computer readable medium, comprising:

a home control application for use in controlling a device, the home control application having a first component executable on a target computer and a second component executable on a remote computer;

a control program operable at the remote computer comprising:

means for issuing a service request;

means for receiving an IP address identifying a network location;

means for registering the IP address to the home control application first component; and

means for controlling the home control application to issue a control command to remotely control the device;

a control program operable at the target computer comprising:

means for switching to a given communications mode;

means for executing a login sequence to an ISP; and

means, responsive to receipt of the control command, for controlling the remote device through the home control application second component; and a control routine operable at the ISP comprising:

means, responsive to the service request from the remote computer, for contacting the target computer;

means for executing the login sequence with the target computer;

means for issuing the IP address; and

means for providing the IP address to the remote computer.

Thus a user may control a target computer from a remote location, through a computer network such as the Internet.

The preferred embodiment provides an access protocol for enabling a user to command a home computer. The remote machine through which the user connects to his or her home PC (ie the target system) may for example be a laptop or other portable computer and this can be used to control a set of devices, e.g., via a smart network such as an X-10 interface. In the preferred embodiment electronic devices in a home are controlled from a remote location using the Internet, but a long distance telephone call or other RF link may alternatively be used. The user may communicate with his or her home computer via the user's Internet Service Provider (ISP). An ISP access protocol is implemented by which a user may establish a remote connection to his or her home computer through the user's ISP. The

BNSDOCID: <WO___0065774A1_I_>

ISP is enabled to contact the user's computer to cause that computer to connect to the Internet so that the computer may receive e-mail or other commands from the user, located elsewhere.

According to the preferred embodiment, to initiate the protocol, the user launches an application which, via the Internet, sends a request to the user's home computer (or other target). If the home computer is not currently connected to the Internet, the user's ISP dials the home computer. The home computer automatically answers, and the ISP sends authentication information to the computer to establish an Internet connection. With the connection established, an IP address for the home computer is sent back to the user at the remote machine, which then can be used to invoke X-10 functions, telnet sessions, or other activities with the target computer. After an explicit disconnect command or timeout, the target computer is disconnected and may be placed into a low power mode. The ISP may charge a nominal fee for this service.

Thus according to the preferred embodiment, a method is described for enabling a remote machine having access to the Internet to control a computer normally connected to the Internet via a service provider. The method begins by initiating a service request from the remote machine to the computer. The service request may be initiated in an e-mail from the remote machine or by having the user visit a secure Web page from which the remote service may be activated. In response to the service request, an Internet connection is established between the ISP and the computer. For example, this connection is established by executing a login sequence between the ISP and the home computer. If the login sequence is successful, the home computer is placed in a given communications mode (e.g., Point-to-Point Protocol (PPP)) and the ISP issues the home computer an IP address. This IP address is also provided to the remote machine. The user of the remote machine uses the IP address to establish a communications path between a home control application executing on the remote machine and on the home computer. The given application may then effect a control function against a given device.

BRIEF DESCRIPTION OF THE DRAWINGS

A preferred embodiment of the present invention will now be described in detail, by way of example only, and with reference to the following drawings:

Figure 1 depicts a conventional client-server information retrieval system used to access the Internet in a known manner;

Figure 2 depicts the remote home computer control system according to a preferred embodiment of the present invention;

Figure 3 is a simplified block diagram of an ISP architecture in which a preferred embodiment of the present invention is implemented;

Figure 4 is a flowchart illustrating a routine for placing a home computer into an operating state from which it may be controlled via a remote machine according to one embodiment of the present invention;

Figure 5 is a detailed flowchart of a first embodiment of the reverse ISP activation system provisioned according to a preferred embodiment of the present invention; and

Figure 6 is a user interface for the remote machine according to a preferred embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is preferably implemented in a known client-server system as illustrated in **Figure 1**. By way of brief background, in this system a client machine **10** is connected to a server **12** via network **14**. For illustrative purposes, network **14** may be the Internet, an intranet, an extranet or any other communications network, and the server is a web server. Web server **12** is one of a plurality of servers which are accessible by clients, one of which is illustrated by machine **10**. The client machine includes a browser **16**, which is a known software tool used to access the servers of the network. The Web server supports files (collectively referred to as a Web site) in the form of hypertext documents and objects. In the Internet paradigm, a network path to a server is identified by a so-called Uniform Resource Locator (URL).

A representative Web server **12** is an IBM Netfinity server comprising a RISC-based processor **18**, the AIX® operating system **20** and a Web server program **22**, such as Netscape Enterprise Server. The server **12** also includes an Application Programming Interface (API) **23** that provides extensions to enable application developers to extend and/or customize the core functionality thereof through software programs including Common Gateway Interface (CGI) programs, plug-ins, servlets, active server pages, server side include (SSI) functions or the like.

A representative Web client is a personal computer that is x86-, PowerPC®- or RISC-based, that includes an operating system such as IBM® OS/2® or Microsoft Windows '95, and that includes a Web browser, such as

BNSDOCID: <WO___0065774A1_I_>

Netscape Navigator 4.0 (or higher), having a Java Virtual Machine (JVM) and support for application plug-ins or helper applications.

Referring now to **Figure 2**, a user having a remote computer **25** can access his or her home-computer **27** via the Internet. As will be seen, according to the preferred embodiment the user accesses his or her home computer **27** (e.g. for the purpose of controlling a device **29** attached to smart network **31** within the home) through the user's own Internet Service Provider (ISP) **33**, although the same service may be offered by another entity (e.g., a dedicated server, another ISP, or the like). ISP **33** includes a server, such as the computer described with reference to figure 1. The user's home computer **27** may control a given device **35**, or the interface (e.g., an X-10 interface) **31** that controls a set of home devices **29**. Representative home devices include, without limitation, lights, a lighting control system, communications equipment, motors, audio/visual equipment, appliances, other computers, HVAC systems and devices, sprinkler systems, security systems, and the like. It will be appreciated that the invention is not limited to control of any particular device, system, component or interface. Moreover, neither is the invention limited to controlling a home computer, but may be used to enable a remote computer user to control a target computer (via the Internet or other computer network) regardless of where the target computer is located.

The remote computer **25** may be a desktop, a laptop, or other portable computer provisioned with suitable devices to connect to the Internet and includes a Web browser. Alternatively, the remote device is a pervasive computing client device, such as a palmtop computer, for example, a device marketed by the IBM Corporation under the WorkPad trademark. Representative devices include a pervasive client that is x86-, PowerPC®- or RISC-based, that includes a runtime operating system such as WindRiver VXWorks™, QSSL WNX4™, or Microsoft Windows CE, and also include a Web browser.

Figure 3 illustrates a conventional Internet operating environment wherein client machines **42** connect to the Internet via an Internet service provider (ISP) **44**. Typically, an Internet service provider **44** provides Internet access to the users for a monthly, yearly or usage-based service fee, or in some cases no fee at all. Thus, for example, a typical Internet service provider charges a given monthly fee to provide a user of a client machine **42** a certain amount of Internet access. According to the preferred embodiment, a client machine user is provided an option to obtain an additional service whereby the user may access his or her home computer (or other target device) remotely through the ISP, even if the

home computer is not then active or currently connected to the ISP or the network. As noted above, this communication path **45** enables the user to control a home device, system or interface from a remote location via the Internet connection established between the ISP and the user's home computer. This communication path is referred to as a reverse ISP connection as, typically, the user connects to the ISP instead of the other way around as described herein. Any fee charged by the ISP for the service may be charged against the user's ISP account.

When a user contracts for his or her Internet service, ISP **44** (if provisioned) offers the reverse ISP activation as an incidental service. The user determines whether he or she desires to accept the service and, if so, whether given limitations are to be placed on the service. Thus, for example, the user may be provided with the option of restricting the number of allowable transactions, perhaps on a per day or per hour basis, or the option of restricting access to the service to certain individuals, by class of service (e.g., based on a self-supplied or third party-supplied rating), or any other such desired restriction.

The user's home computer is accessed through the Internet according to the reverse activation protocol described herein. As will be seen, there are several different techniques that may be used to access the user's home computer from the remote location. Regardless of the access method selected, it is preferred that the home computer be powered on but be in a low power or standby mode of operation. **Figure 4** is a simplified flowchart of a routine for accomplishing this functionality at the home computer. This routine assumes that there is no live network connection between the home computer and the ISP. As will be seen, the ISP (or other service provider) establishes a connection to the user's home and wakes-up the user's home computer to enable the user to remotely control the computer through a reverse ISP connection.

In one embodiment, the user sets the home computer's modem to an automatic answer mode of operation at step **50**. At step **52**, the user opens an e-mail client which is used to listen for an e-mail that includes control or operating instructions for the home device, system or interface to be controlled. Step **52** may be omitted if e-mail command operations are not required (e.g., if the user controls the home application via a secure Web page ISP connection, as will be described). At step **54**, the user starts a home control application that is used to perform a given management, monitoring or control function for the home device, system or interface. Alternatively, the home control application is started later after the

BNSDOCID: <WO___0065774A1_I_>

user accesses the home computer from the remote location, as will be seen. Of course, the sequence of the above steps may be varied.

As will be seen, once the ISP establishes an active connection to the home computer, the user at the remote machine uses the home control application to effect the monitoring or control function. At step **56**, the application listens on a given sockets port (whenever a TCP/IP connection between the client and the ISP is established) to determine whether a communications pathway has been opened. Alternatively, a local proxy server (in the home computer) can be used to shield the application from having knowledge of whether the TCP/IP connection is up or down. At step **58**, the routine continually tests for an interrupt appearing on the modem serial port. Upon receipt, the client machine is powered up at step 59 and is now in a condition to be controlled from the remote location via the reverse ISP activation service.

Figure 5 is a simplified flowchart of the reverse activation protocol of the preferred embodiment. The user of the remote machine initiates a connection to the home computer by visiting a secure Web site (e.g., a Web site operated by, on behalf of, or for the benefit of, the ISP, or some third party). The routine begins at step **60** with the user of the remote machine navigating to the secure Web page (e.g., via secure sockets or https: connection). From this page, the user enters a userid and password, indicating that he or she desires to perform a reverse activation. At step **62**, the ISP calls the home computer and, optionally, sends given login information (e.g., userid and password). At step **64**, the home computer, which has been setup to wait for such a call, answers with its modem. For example, step **64** generates an interrupt on the modem's serial port. The modem (or other routine) may also discriminate the signal to ensure that the incoming call is a data call (as opposed to voice or a fax). If the home computer does not answer within a given time, an error message is sent to the user at the remote machine (not shown). If the modem answers, the home computer goes from a standby to a normal mode of operation. At step **66**, the client routine authenticates the ISP call. The routine then continues at step **68** with the home computer switching to a PPP connection mode, during which the computer logs into the ISP in the usual manner. Alternatively, the home computer hangs up the connection and calls back the ISP to initiate the PPP connection.

Control then shifts to the ISP where, at step **70**, the ISP accepts or rejects the home computer's PPP login. On the client, the control routine

running on that computer activates the home control application (step **69**). Alternatiely, that application may have already been started by the user at some earlier time, as previously described. Back at the ISP, the routine assigns the home computer an Internet Protocol (IP) address, which is then sent to the remote machine (step **72**). At step **74**, the remote machine operating routine registers the client IP address for a remote end of the home control application, which is also running on the remote machine. At step **76**, the home control application initiates a request to control a given device, an interface, or the like, at the home. At step **78**, the home control application running on the client controls the device or interface (as the case may be) as per the user's request. If the control function cannot be carried out within a given timeout period at step **80**, the routine disconnects the home computer from the ISP at step **82**. This completes the processing.

Figure 6 illustrates a representative user interface for the home control application running on the remote machine according to the preferred embodiment. Of course, this interface is merely illustrative of the functionality. As can be seen, the interface control includes a panel identifying each of the controlled devices. In this example, the front outside lights may be positioned on or off, and the current operating condition is illustrated as off. The rear outside lights are in a similar condition. The television is identified as being currently on and tuned to Channel 7. The air conditioning unit is off, with the indoor temperature at 74 degrees and the outdoor temperature at 80 degrees. The security system is shown as armed and at a nominal operating status. The kitchen appliances are off. A live video shot, for example, of the user's living room, is also available from the interface. One of ordinary skill will readily appreciate that, using this remote interface, various operating conditions of these devices and systems may be readily monitored or changed as desired. Further, if the remote machine is a pervasive computing device, such as a portable wireless computer, the user can control the various device settings whilst he or she is on the move (eg driving home, using public transport etc).

As noted above, the particular purpose or operation of the home computer application is not limited. Thus, for example, the application (or one or more applications) may be used to control a lighting system, to control a sprinkler system, to control a video camera to feed video frames, to activate a heating or cooling system, to open a garage door, to activate a lock, to initiate a security scan, or any other type of activity that the user desires. In the preferred embodiment, the user of

BNSDOCID: <WO___0065774A1_I_>

the remote machine connects to his or her home computer to invoke X-10 functions, telnet sessions or other activities with the client machine. After an explicit disconnect command or timeout, the home computer is disconnected and may be powered down into a low power mode as previously described.

Thus, in the preferred embodiment, the user at the remote machine navigates to a secure Web page and initiates a connection to the target computer. If security is not a concern, alternate techniques may be used to initiate the connection. Thus, for example, another way of initiating the request for the service is for the user (at the remote machine) to transmit an e-mail to the home computer, perhaps with a special character string that is recognized by the ISP e-mail server. This e-mail may be a request for the service, or it may include an actual command string of information for controlling the home control application. Of course, the command string may itself be used to start a given application on the client machine. In this embodiment, once the client logs into the ISP (as previously described), the ISP assigns the client an IP address, which is then returned to the remote machine for use by the home control application executing on that machine.

Many other variations are within the scope of the present invention. Thus, as briefly mentioned above, once the ISP verifies itself to the home computer, the initial connection between the ISP and the home computer may be dropped (i.e. terminated). At this point, the home computer is controlled (through a control program) to dial the ISP normally (through its native dialup networking capability) and present itself for connection to the ISP in the usual manner. Once this connection is established, a message is returned to the remote machine, which may then establish a socket to the application in the manner previously described. This technique is somewhat more secure than the technique described above but requires two connections instead of one. In either case, the ISP makes a call and wakes up the home computer so that the user of the remote machine can control a local application.

The control routines described above are distributed across the remote machine, the ISP, and the home (or other target) computer or device. The routines are implemented as a set of instructions (computer program code) in a code module resident in or downloadable to the random access memory of a computer. Until required by the computer, the set of instructions may be stored in another computer memory, for example, in a hard disk drive, or in a removable memory such as an optical disk (for

eventual use in a CD ROM) or floppy disk (for eventual use in a floppy disk drive), or downloaded via the Internet or other computer network.

In addition, although the various methods described are conveniently implemented in a general purpose computer selectively activated or reconfigured by software, one of ordinary skill in the art would also recognize that such methods may be carried out in hardware, in firmware, or in more specialized apparatus constructed to perform the required method steps.

BNSDOCID: <WO___0065774A1_I_>

CLAIMS

1. A method for enabling a remote machine (25) having access to a computer network (14) to control a computer (27) normally connected to the network via a service provider (33), comprising the steps of:

initiating a service request from the remote machine to the computer (step 60);

responsive to the service request, establishing a network connection between the service provider and the computer; and

controlling the computer from the remote machine over the network connection (steps 76, 78).

2. The method as described in Claim 1 wherein the step of establishing the network connection includes:

executing a login sequence between the service provider and the computer (steps 68. 70);

if the login sequence is successful, placing the computer in a given communications mode;

issuing a network address to the computer;

forwarding the network address to the remote machine (step 72); and

establishing a communications path between the remote machine and the computer.

3. The method as described in Claim 1 wherein the step of establishing the network connection comprises:

executing a login sequence between the service provider and the computer;

if the login sequence is successful, terminating a connection between the service provider and the computer (step 82); and

initiating a connection between the computer and the service provider using the computer's native dialup networking mechanism.

4. The method as described in Claim 1, wherein the remote computer and the computer under control are connected to the Internet, said method comprising the steps of:

initiating a service request from the remote machine to the computer over a secure connection;

initiating a login sequence from the home computer to the ISP;

issuing an IP address to the home computer;

returning the IP address to the remote machine; and

controlling the computer from the remote machine over the Internet connection (steps 76, 78).

BNSDOCID: <WO__0065774A1_I_>

5. The method as described in Claim 4 wherein the step of controlling the computer from the remote machine includes establishing a communications path between the remote machine and the computer.

6. The method as described in any of Claims 2 to 5 further including the step of authenticating the user prior to initiating the login sequence (step 66).

7. The method as described in any preceding claim, wherein the step of controlling the computer from the remote machine includes:

receiving at the computer a control command issued from the remote machine; and

responsive to the control command, initiating a command function against a given device.

8. The method as described in Claim 7 wherein the given device is a home control interface.

9. The method as described in Claim 7 or 8 wherein the control command is issued with the service request.

10. The method as described in Claim 7 or 8 wherein the control command is initiated after the network connection is established.

11. The method as described in any preceding claim wherein the service request is initiated from a secure Web page associated with the service provider.

12. The method as described in any preceding claim wherein a given fee is charged against a user's service provider account for the service request.

13. The method as described in any preceding claim wherein the service request is initiated by transmitting an e-mail from the remote machine.

14. A computer (25) connectable to an Internet Service Provider (ISP) (33) for remotely controlling a device (29, 35) in a home, comprising:

a processor;

a home control application including means for generating a display interface for use in controlling the device; and

a control program executed by the processor comprising:

means for issuing a service request;

BNSDOCID: <WO___0065774A1_I_>

means for receiving an IP address identifying a network location;

means for registering the IP address to the home control application; and

means for controlling the home control application to issue a control command to remotely control the device.

15. A computer (27) connectable to an Internet Service Provider (ISP) (33) for controlling a device (29, 35) in a home, comprising:

a processor;

a modem;

a home control application for controlling the device; and

a control program executed by the processor comprising:

means, responsive to an interrupt at the modem, for switching to a given communications

mode;

means for executing a login sequence to the ISP; and

means, responsive to receipt of a control command, for controlling the remote device

through the home control application.

16. A computer operable at an Internet Service Provider (ISP) (33), comprising:

a processor;

a control program executed by the processor comprising:

means, responsive to a service request from a remote computer, for contacting a target computer;

means for executing a login sequence with the target computer;

means for issuing an IP address to the target computer if the login sequence is successful; and

means for providing the IP address to the remote computer to enable a user of the remote computer to control a device associated with the target computer.

17. A computer program product in a computer readable medium, comprising:

a home control application for use in controlling a device, the home control application having a first component executable on a target computer (27) and a second component executable on a remote computer (25);

a control program operable at the remote computer comprising:

means for issuing a service request;

means for receiving an IP address identifying a network location;

means for registering the IP address to the home control application first component; and

means for controlling the home control application to issue a control command to remotely control the device;

a control program operable at the target computer comprising:

means for switching to a given communications mode;

means for executing a login sequence to an ISP; and

means, responsive to receipt of the control command, for controlling the remote device through the home control application second component; and

a control routine operable at the ISP comprising:

means, responsive to the service request from the remote computer, for contacting the target computer;

means for executing the login sequence with the target computer;

means for issuing the IP address; and

means for providing the IP address to the remote computer.

18. The computer program product as described in Claim 17 wherein the smart network (31) interface is an X-10 interface.

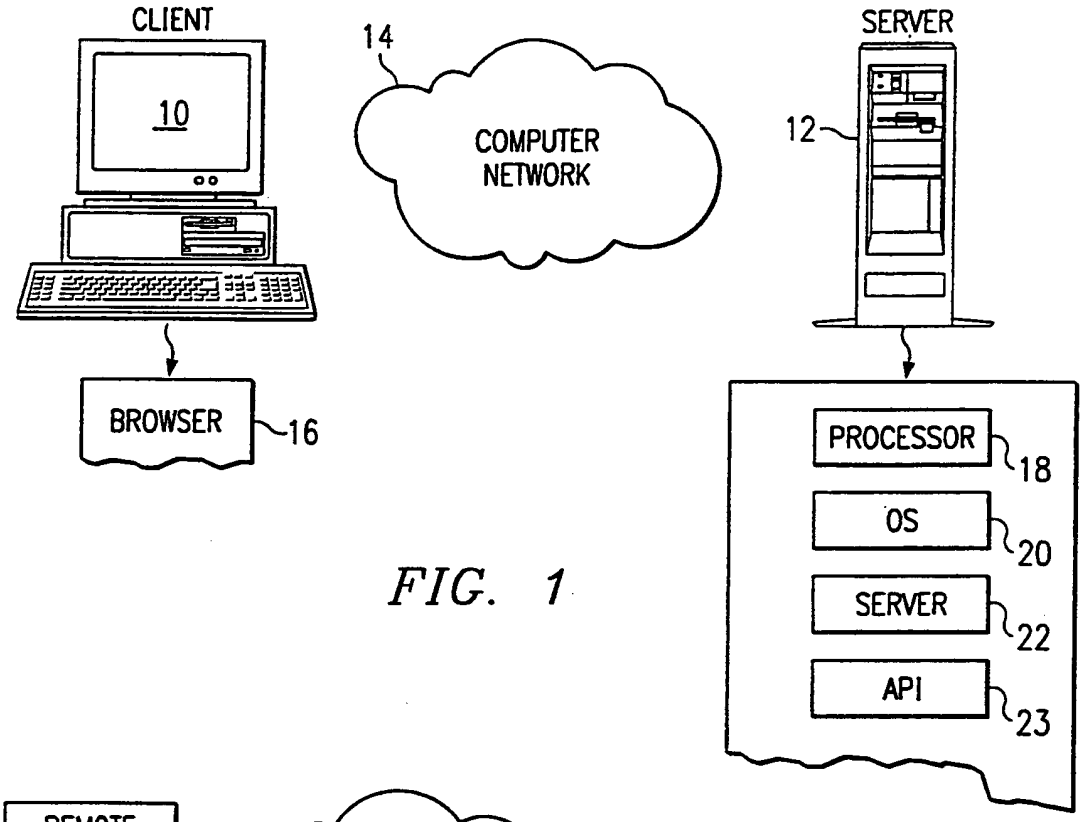


FIG. 1

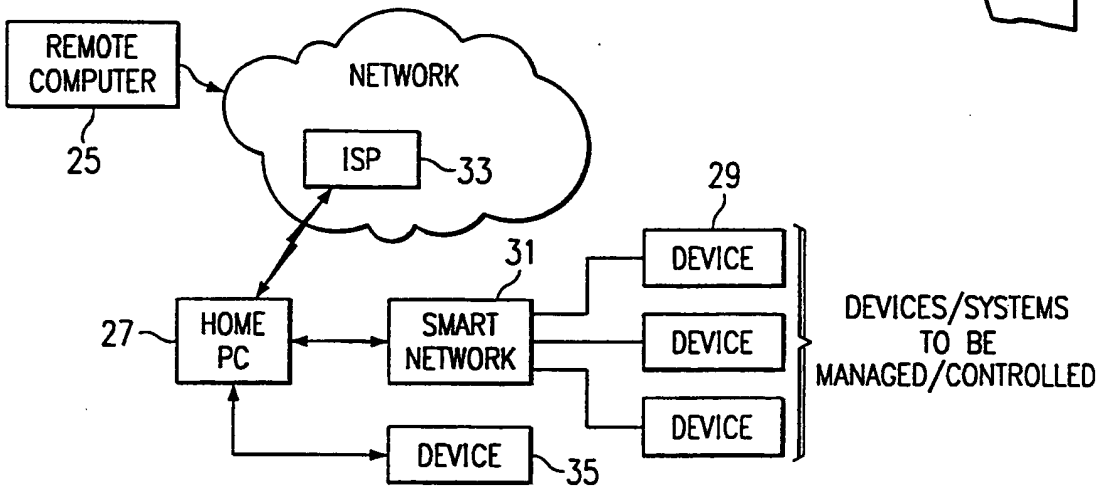


FIG. 2

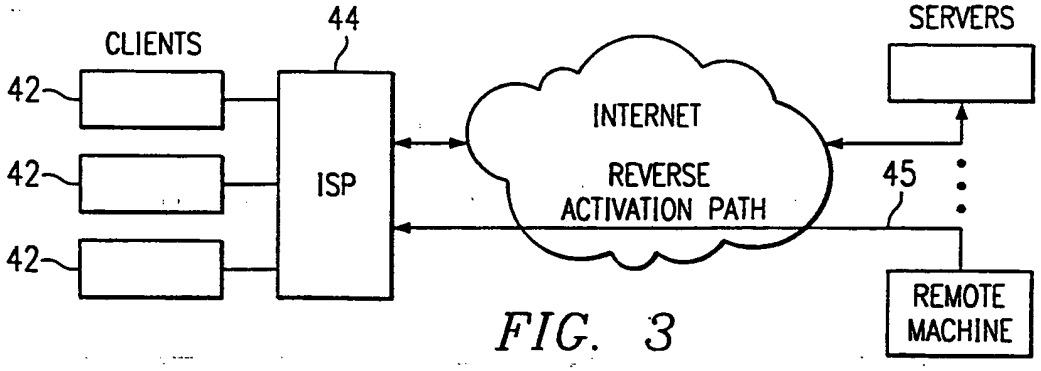


FIG. 3

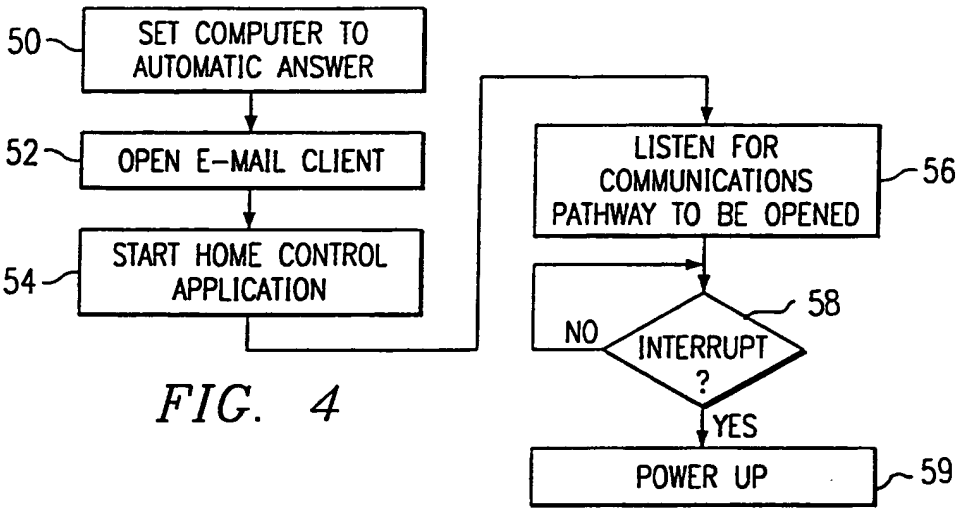


FIG. 4

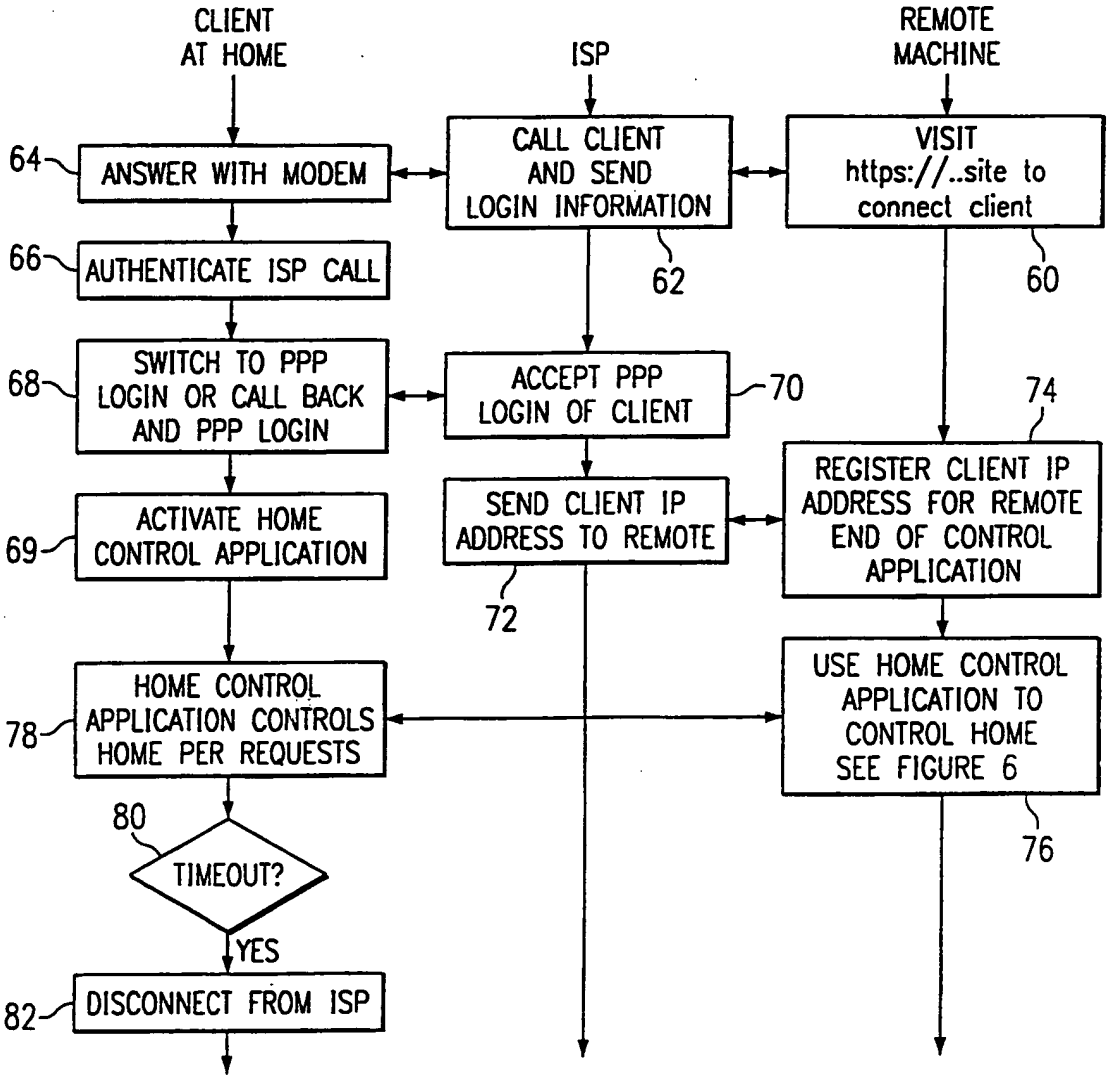


FIG. 5

BNSDOCID: <WO___0065774A1_I_>

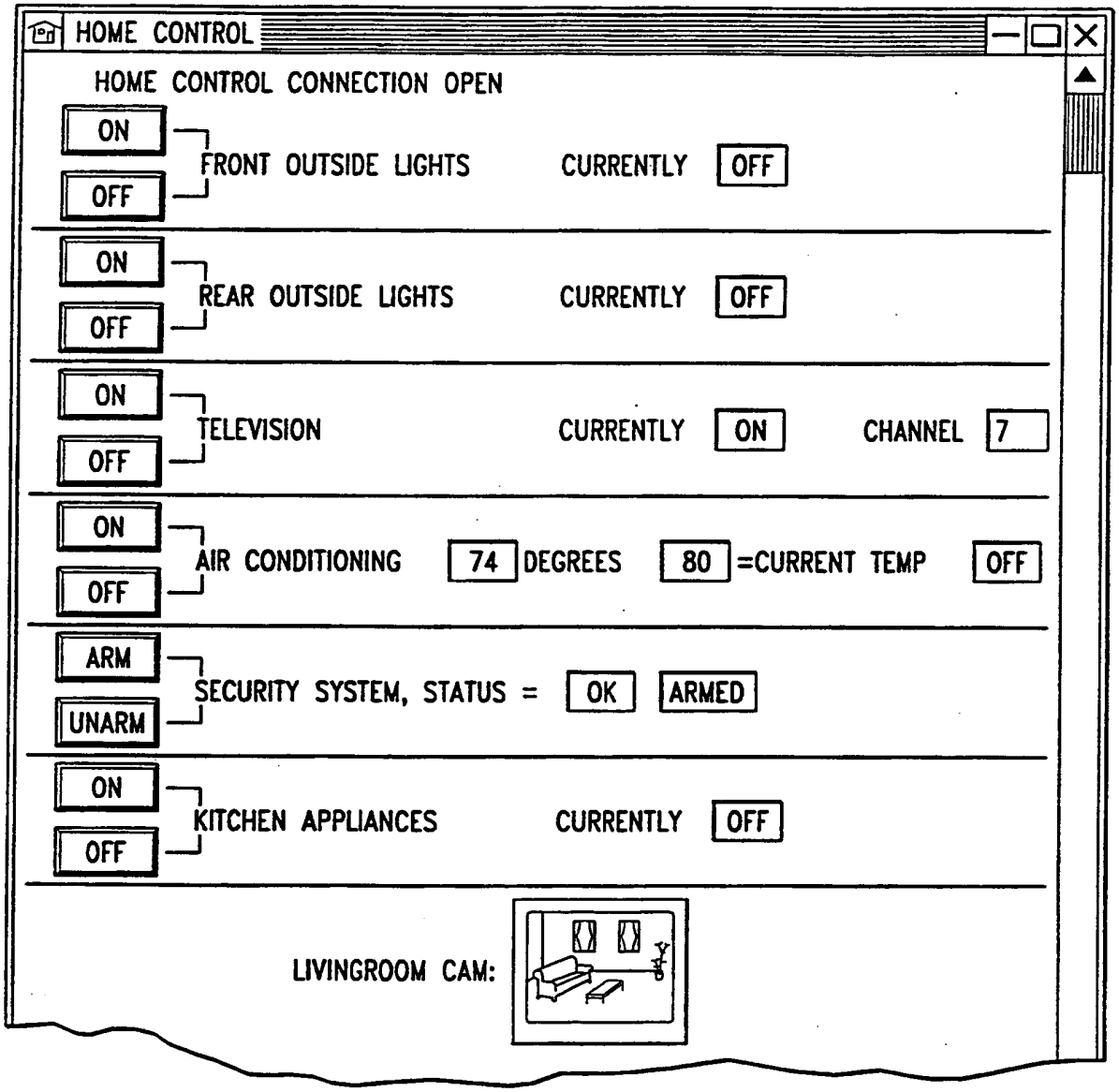


FIG. 6

BNSDOCID: <WO___0065774A1_I_>

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 00/01465

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/12 H04L29/06 G06F9/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	US 5 949 412 A (HUNTSMAN ROBERT A) 7 September 1999 (1999-09-07) abstract column 1, line 10 - line 15 column 2, line 67 - line 13 column 4, line 5 - line 31 column 8, line 22 -column 10, line 29	1,14-17
P,X	EP 0 943 992 A (IBM) 22 September 1999 (1999-09-22) abstract page 2, column 1, line 29 - line 57 page 5, column 8, line 1 - line 44	1,14-17

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 October 2000	10/10/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Adkhis, F

1

Form PCT/ISA/210 (second sheet) (July 1992)

BNSDOCID: <WO__0065774A1_I_>

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 00/01465

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
P,X	DE 197 37 651 A (RIEMANN FRANK) 6 May 1999 (1999-05-06) abstract page 2, line 23 - line 35 page 3, line 59 -page 4, line 4 page 5, line 67 -page 6, line 3	1,14-17

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

BNSDOCID: <WO___0085774A1_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 00/01465

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5949412 A	07-09-1999	US 5801689 A	01-09-1998
EP 0943992 A	22-09-1999	US 6085227 A	04-07-2000
		CN 1229956 A	29-09-1999
		JP 11328080 A	30-11-1999
DE 19737651 A	06-05-1999	NONE	

BNSDOCID: <WO___0065774A1_I_>

THIS PAGE BLANK (USPTO)